Information rights report
Quarter 3 - 2015/16

Contents

1. Cross Sectoral Work

1.1 Good Practice

In accordance with our obligations regarding SIS II, we completed an audit of the Sirene Bureau at NCA and are undertaking a corresponding audit of the Home Office Live Police Systems in early January 2016.

We continue to deliver the programme of workshops with Local Medical Committees specifically targeted at providing General Practitioners and their Practice Managers with practical Data Protection (DP) advice.

We organised and ran a DP workshop in London specifically for the members of the Victims Service Alliance which was well received.

The Communications Audit Team has completed its first site visit to a CSP that is subject to a data retention notice. The team has continued to liaise with a number of other CSPs regarding site visits planned under the Data Retention and Investigatory Powers Act (DRIPA) for Q4 and has also been preparing for the ICO's future audit responsibilities under the Draft Investigatory Powers Bill.

2. Government and Society Sector

2.1 Data sharing proposals, including possible legislation

Redacted

2.2 Government databases and digital services

The Government Digital Service (GDS) in the Cabinet Office is aiming to reform silo working across government by developing a platform-based approach to IT. The Chancellor announced significant investment in digital technology in the recent spending review. GDS are working on an open, common IT architecture to increase transparency and transform the way the government does business. As part of this they want to make better use of data across central and local government decision making, and support simpler and faster services for citizens. A key element will be the need for greater data sharing.

The GOV.UK Verify identity assurance programmed continues to be rolled out. This allows individuals to identify themselves when accessing online government services using a third party identity provider. There are now 317k registered users; expected to expand to over 1m during the year. Thirteen services are currently available from viewing your own DVLA driver record to competing HMRC self-assessment returns. A further ten services will be added by April.

There are currently four private sector identity providers; increasing to nine this month. The autumn spending settlement resulted in secured funding up to 2020 to ensure the continued roll out.

We continue to participate in the Privacy and Consumer Group that works with the Cabinet Office on the privacy aspects of the programmed. We participated in a very positive meeting with Matthew Hancock, Cabinet Office Minister, to discuss the work and necessary privacy safeguards.

Outcome:

Our constructive engagement is ensuring that we are involved in these new developments. DP and privacy safeguards are increasingly viewed as essential elements of new developments and this has been reflected in positive Ministerial comments.

Future work:

We continue to participate in government discussions and will attend an event on 11 February 2016 which will launch the Government's digital strategy for the next four years. We shall continue to participate in cross-government meetings, for example attending the Verify Privacy and Consumer Group. We are meeting the newly appointed Privacy Officer for Verify on 13 January. We shall also continue to participate in a cross-government group looking at tackling misleading websites

Contact: Judith Jones, Richard Marbrow, Jonathan Bamford (for Verify PCAG)

2.3 HMRC employment history subject access requests

Redacted

2.4 Political parties and campaign groups

The EU Referendum Bill received Royal Assent in December so the referendum can take place between now and the end of 2017. With strong indications that it could take place this year, campaigns groups are forming and the office has already started to receive complaints.

Outcome:

To be proactive we published a blog on 6 January 2016, reminding campaign groups and political parties that they must comply with the law.

Future action:

We shall monitor any concerns and take enforcement action where appropriate.

Contact: Judith Jones

2.5 Re-use of government databases for wider purposes

Redacted

3. Police, Justice and Borders Sector

3.1 Police use of surveillance technologies

Redacted

3.2 Metropolitan Police Service (MPS) – Information Rights Performance

Redacted

3.3 Draft Investigatory Powers Bill

The Draft Investigatory Powers Bill has been published. The ICO provided a written submission to the Joint Committee considering it providing details of our key concerns about the provisions, our experience of auditing retained communication data and the value to our own enforcement work in having access to this data. The Commissioner also gave evidence in person on 6 January.

We continue to have audit responsibilities over communication service providers (CSPs) but have asked for clearer strengthened powers to undertake this role. We also provided written evidence to the Commons Science and Technology Committee as part of its inquiry into the technology and security aspects of the Bill on CSPs.

Outcome:

A very detailed submission covering the key relevant points was submitted to the Joint Committee which were expanded upon by the Commissioner in his oral evidence.

Future work:

The Bill will be on a tight timescale potentially entering Parliament in late spring. We expect detailed work with the Home Office particularly on the provisions affecting the ICO. This may include additional funding if our audit work extends to retained internet connection records and data retained by overseas CSPs

Contacts: Jonathan Bamford, Steve Wright, Steve Dickenson, Ian Deasha

3.4 Prüm Decision

Redacted

4. Public Services Sector

4.1 Changes to legislation

Significant changes to health sector regulations, the introduction of the Cities and Local Government Devolution Bill, Immigration Act, the Health and Social Care Act (Safety and Quality) plus the proposed creation of the Office of the National Data Guardian (NDG) all have impacts on information rights. This includes our own regulatory relationship with the NDG.

Outcome:

Increased involvement with the relevant stakeholders who are, or have, drafted the legislation, and with those who are being expected to implement it, has enabled us to identify policy developments and assist in highlighting the information rights impacts and considerations which need to be taken into account. We have submitted consultation responses when appropriate. Our independent input has been welcome. The contacts we are developing in these arenas are becoming invaluable to the work of the office generally as they provide a point of reference for other intelligence and information. It is also allowing us to better understand the long term plans and strategies of government departments in relation to public services information management and particularly data sharing.

Future work:

We will maintain close working relationships with Department of Health, NDG, Greater Manchester authorities and others to enhance understanding.

We will continue to monitor progress and identify and influence key aspects and impacts.

Contact: Dawn Monaghan, Andrew Rose, Victoria Cetinkaya

4.2 Sectoral standards, codes and polices

There is presently a plethora of standards, codes and policies being developed in the public sector in relation to information governance (IG). These include information and anonymisation standards in Health and Social Care, updates to the IG toolkit, a review of information security and many others.

Outcomes:

We identified the main items of work and ensured we have had access to draft copies, and where appropriate, involvement in their development to influence any approaches which may deviate from an ICO policy view or interpretation of the laws we regulate.

Future Work:

There will be continued involvement with stakeholders in the areas of work already undertaken. We will also monitor future proposals.

Contact: Victoria Cetinkaya, Sarah Clements, Stacey Egerton

4.3 Sectoral Data Sharing Initiatives

The present trend for increased data sharing to facilitate public sector transformation and integrated care continues. Projects such as Care. Data and Troubled Families are national policies, but there are now numerous regional area multi-agency sharing initiatives for which we are providing advice.

Outcome:

We have increased contact with and input into work by the Local Government Association, Information Governance Alliance, Pioneer Programme Board and Centre of Excellence for Information Sharing. We have successfully secured observer status at the new Strategic Oversight Panel chaired by Lord Darzi. Working with the above stakeholders, we have addressed key areas of concern and have identified ways of providing guidance and assistance to organisations which incorporate the views of the ICO.

Future Work:

We will be working with key stakeholders to continually monitor and identify areas of concern and improvement and to identify good practice.

We will be encouraging representative bodies to produce sector specific guidance which incorporates our views. We will continue attending relevant panels and boards.

Contact: Dawn Monaghan, Stacey Egerton, Andrew Rose, Sarah Clement

4.4 Strategic and Technological Developments

Several high level projects which are in development or implementation stage require consideration and constant monitoring. These include 999 Eye, Electronic Prescription Service, On-line Access to GP records, genomics and medical apps.

Outcome:

Public sector stakeholders who are leading these initiatives have been contacted, relationships have been built and regular meetings held to ensure influence is brought to bear.

Future work:

We will continue to meet stakeholders and feed into the production of documentation and respond to consultations as appropriate.

Contact: Victoria Cetinkaya, Dawn Monaghan

4.5 Notification of Nurses and Midwives

The Nursing and Midwifery Council approached us about its strengthened rules requiring professional revalidation of nurses and midwives by third parties and concerns that these third parties would be data controllers if they retained the information electronically leading to 700,000 nurses and midwives having to register with the ICO or retain the information and submit it in paper form. We discussed the matter with the Council and clarified our regulatory approach that, although there is no relevant exemption we are not contemplating action for non-notification.

Outcome:

The Council amended its guidance to nurses and midwives to reflect the ICO line, moving away from saying that such details must be held in paper form or notification would be required

Future action:

We have raised the issue and the need for a non-notification exemption with DCMS. Changes to notification under the EU General DP Regulation will mean that such a liability is unlikely in the future. In the meantime we will be maintaining contact with the Council over any concerns from nurses and midwives.

Contact: Jonathan Bamford, Victoria Cetinkaya, Steve Wood

5. Business & Industry Sector

5.1 National data breach protocol

Redacted

5.2 Microsoft Windows 10

Redacted

5.3 Open Banking Working Group

The Open Banking Working Group was established to deliver on the government's commitment to publish a plan for the creation of an open Application Programming Interface standard for bank data. It completed its report on schedule at the end of 2015. This report is currently being considered by HM Treasury prior to publication. A number of regulatory concerns and risks were identified in the report, including the potential impact of the General DP Regulation and the forthcoming second Payment Services Directive (PSD2) which will place mandatory requirements on some organisations to disclose financial transaction data. Some of the DP concerns, for example conditions for processing sensitive personal data, have yet to be resolved.

Outcome:

We participated in the work of the regulatory and legal sub-group, providing advice and guidance on where the ICO's concerns may lie.

Future work:

It is inevitable that the ICO will be called upon to give further guidance as this initiative develops.

Contact: Garreth Cameron

5.4 Big data

The Financial Conduct Authority (FCA) has published a call for evidence on the use of big data in the general insurance sector. The call focuses on whether big data affects consumer outcomes, fosters or constrains competition, and whether their regulatory framework affects developments in big data in retail general insurance. The FCA's interest in big data within the context of retail general insurance is welcomed, and it is hoped that their work will help

develop our own thinking, in particular when considering fairness of processing.

Outcome:

Utilising our relationship with the FCA, we were in a position to discuss their proposal for work in this area at a relatively early stage. We were able to advise on those areas we considered important and worthy of further exploration, drawing upon what we have learnt from our recent workshops with the insurance industry on the use of PIAs in a big data context. We have submitted a formal response.

Future work:

We will review the response to the call for information and liaise further with the FCA to see how we might usefully collaborate on this issue.

Contact: Alastair Barter, Garreth Cameron, Carl Wiper

5.5 Electronic Identification and Trust Services (eIDAS) Regulations

Redacted

5.6 Cyber Security

The Culture, Media and Sport Parliamentary Committee is undertaking an inquiry into cyber security and the protection of personal data online. This follows on the back of the well-publicised Talk Talk security breach.

Outcome:

We provided written evidence to the Committee covering our work around cyber security including enforcement action around breaches. We renewed our call for custodial sentences for s.55 offences. The evidence also covered security issues arising from the requirements on communication service providers to retain data under the Investigatory Powers Bill.

Future work:

The Commissioner has been asked to appear before the Committee on 27 January to give oral evidence.

Contact: Abi Saul (written evidence), Jonathan Bamford (IP Bill concerns) Simon Rice (oral evidence session)

6. National Regions

6.1 Wales

6.1.1 Local government

In the light of future local government reorganisation in Wales we have continued our programme offering local authorities an 'open agenda' meeting with the ICO. The aim is to establish an up-to-date network of local authority contacts with a view to helping them prepare for the planned changes. We will also share learning with them from the ICO's involvement with councils in NI during their own recent reorganisation.

Future work:

A number of meetings have now been scheduled for the coming months.

Contact: Dave Teague

6.1.2 ICO Wales Conference 2015

In November we ran a DP conference in mid-Wales, aimed at IG professionals across all sectors in Wales. The event included keynote presentations and interactive breakout sessions covering PIAs, our approach to enforcement and European and international developments. Several staff from other ICO offices also took part.

Outcome:

The event was fully booked with over 120 delegates attending. Feedback was overwhelmingly positive, with networking opportunities and the chance to speak directly to a number of ICO staff being very much appreciated.

6.1.3 Schools and children

In the quarter we ran three regional workshops with the Wales Pre-school Providers Association, raising awareness of basic DP requirements with small businesses providing childcare. We also ran the first two of our new half day workshops on the DPA and FOIA with school governors in Wrexham and Denbighshire. All the workshops were very well received.

Future work:

In the coming quarter we will be running the school governor workshop in Bridgend and Merthyr, and a Pre-School Providers Association session in Blaenau Gwent.

Contact: Helen Phillips

6.1.4 PECR work and nuisance calls

Get Safe Online and Welsh police services ran a pop-up shop in Cardiff city centre to raise public awareness about the risk of scams and nuisance calls. We took part, and provided leaflets about our PECR work and how to report unsolicited messages and calls.

Outcome:

In one day we spoke with around 300 members of the public, many of whom were receiving nuisance calls and were very pleased to know how and where to report them.

Future work:

Following this event, we have arranged for the Chief Executive of Get Safe Online to take part in next years' DPP conference.

Contact: Dave Teague, Helen Phillips

6.1.5 IG Training in NHS Wales

The ICO's report on standards of IG training for NHS Wales staff was published in July 2015.

Outcome:

Following publication the NHS Wales Information Governance Management Advisory Group (IGMAG) has commenced two projects. Firstly, it is exploring how to develop a new IG assessment toolkit that is more thorough, requires organisations to provide evidence and will be externally audited. This is likely to be based on England's NHS IG Toolkit and adapted to fit NHS Wales. This approach would also assist with IG assurance for cross border information sharing with NHS England. Secondly a sub-group is reviewing the on-line IG training package, looking at how to provide more targeted training for different professional groups.

During the quarter we met with Wales' Chief Medical Officer, Dr Ruth Hussey, to discuss the report. Dr Hussey was very interested

in the report's findings and had already sent a Welsh Health Circular to NHS Wales' Chief Executives asking for their response to the findings – we later provided some anonymised briefing material to Welsh Government for her meeting with the Chief Executives to discuss their responses.

Future work:

We continue to work closely with IGMAG and the Welsh Government to support improving IG oversight and training in NHS Wales.

Contact: Helen Phillips, Anne Jones

6.2 Northern Ireland

6.2.1 NICVA Information Rights Strategy

In conjunction with the Northern Ireland Council for Voluntary Action (NICVA), we have developed a bespoke programme of events which will be delivered over the course of the next year. The programme incorporates key information rights related topics and interactive workshops designed to promote awareness and compliance right across the voluntary sector.

Future action:

The delivery of a monthly workshop to various organisations within the voluntary sector, covering topics such as DP for charities; direct marketing and PECR; anonymisation, FOI and open data.

Outcomes:

Improved information rights awareness and compliance throughout the sector.

Contact: Shauna Dunlop, Rachael Gallagher

6.2.2 Embedding privacy by design across public sector bodies

Engagement with several public sector bodies and the issuing of advice on conducting PIAs on a number of initiatives including the implementation of new legislation within the NI Ombudsman's Office and the use of new technology within the Department of Agriculture and Rural Development and the PSNI.

Future action:

To provide good practice advice on completed PIAs.

Outcomes:

To enable the public sector to design new initiatives, policies and legislation and use new technology in a way which takes account of privacy from the outset.

Contact: Rachael Gallagher

6.2.3 DP Compliance within the Health Sector

The ICO issued advice to the Access to Healthcare Services team within the NI Business Services Organisation (BSO) on DP compliance relating to a new initiative to screen new patients registering for GP services. The screening will assist with the detection of fraudulent registrations by individuals who reside in Southern Ireland, claiming health care services in Northern Ireland.

Future work:

We have been asked by the BSO for policy advice on DP compliance relating to similar situations within hospital care.

Outcome:

Improved practice with DP requirements relating to detection of fraud and the management of patient information.

Contact: Shauna Dunlop

6.2.4 Law Society of Northern Ireland – Risk Management Conferences

Completion of a 12 month tailored and bespoke programme for the legal profession across Northern Ireland. A further four sessions was delivered to solicitors across NI on DP risk management, attended by approx. 200 solicitors.

Future work:

No specific future work planned although keeping in contact with the Law Society.

Outcome:

Enhanced awareness in the legal sector regarding information rights and the work of the ICO.

Contact: Rachael Gallagher, Shauna Dunlop

6.3 Scotland

6.3.1 Health & Social Care Integration

As the programme of integration of Adult Health and Social Care required under the provisions the Public Bodies (Joint Working) (Scotland) Act 2014 moves closer to 'going live' in April 2016, the ICO's Scotland Office is increasingly being asked to provide advice and guidance to NHS Scotland and Scottish local authorities in relation to DP issues surrounding the delivery models adopted. The majority of areas have adopted a model which requires the establishment of an Integrated Joint Board with representation from the local authorities and the Health Board. This has implications for data controllership and much of the discussion has been around this issues. As well as meetings at a local level, speakers from ICO have delivered talks on the subject to a number of national conferences.

Future action:

Collaborating with the ICO's Legal Team to provide the ICO's view on the data controller status of the various organisations involved in the integration programme. Meeting with key stakeholders to convey the ICO's view and to provide assistance and guidance where necessary. Continued speaking engagements to wider audiences to disseminate the DPA obligations on the existing and new institutions.

Outcome:

Increased awareness and credibility of the ICO as regulator and source of authoritative advice and support.

Contact: Maureen Falconer

6.3.2 Information Sharing Across the Public Sector

Between the establishment of the Named Person under the Children & Young People (Scotland) Act 2014 and the Public Bodies (Joint Working) (Scotland) Act 2014, information sharing is dominating the agenda on the conference circuit as well as exercising the minds

of practitioners and service providers. It is the single biggest issues with the Scottish public sector at this time. The ICO has provided, and continues to provide, speakers for conferences, seminars and organisational awareness sessions on the safe and secure sharing of personal and sensitive personal data in compliance with the DPA. We also participate in a variety of working groups associated with the implementation of the Named Person scheme where we are perceived as providing authoritative yet pragmatic advice to organisations and practitioners trying to ensure compliant implementation of the provisions of both Acts. In addition, this issue is generating an increasing amount of written guidance on which the Office is being consulted.

Future action:

Continued participation in conferences, seminars and workshops to provide practical advice and guidance to ensure compliance. Continued consultation responses to draft guidance documents.

Outcomes:

Increased awareness of the DP requirements in respect to information sharing. Increased awareness and credibility of the ICO as regulator and source of authoritative advice and support.

Contact: Maureen Falconer

6.3.3 DP Awareness for the Third Sector

The voluntary sector is a difficult sector with which to engage given the disparate activities and organisational structures involved. The ICO has been working with a number Councils for Voluntary Services to provide DP workshops to representatives from a variety of Third Sector organisations in different localities across Scotland. These half-day interactive workshops are very well received and appreciated by those attending and who are then tasked with being 'DP Champions' within their own organisations!

Future action:

Continued collaboration with CVS organisations to organise the provision of workshops to provide practical advice and guidance to ensure good information rights practice across the Third Sector.

Outcome:

Increased awareness of information rights and DP obligations. Increased awareness and credibility of the ICO as regulator and source of authoritative advice and support.

Contact: Maureen Falconer

6.3.4 Engagement with religious and philosophical associations

This project has continued with three strands of work. We began with giving the Church of Scotland advice on what it would be beneficial to include in tailored subject access guidance for presbyteries (as data controllers) and the constituent parishes. We also attended a meeting of the Scottish Churches Committee which comprises senior administrative officers from twelve Christian denominations in Scotland, as well as the Scottish Churches Parliamentary Office. Our input highlighted some of the DP concerns relating to churches that had come to our attention and offering guidance and support to improve practices. Finally, in conjunction with the Bishops Conference of Scotland, we facilitated a DP workshop for dioceses and national agencies of the Roman Catholic Church in Scotland with 17 bodies in attendance.

Future work:

At least one further national DP workshop with the Roman Catholic Church is expected to be held in spring 2016, with possible additional work with individual data controllers. We will provide comment on draft guidance by the Church of Scotland on dealing with SARs. A meeting with the Chief Executive of the Free Church of Scotland is to be arranged for early 2016.

Outcomes:

Data controllers recognising the need for clear policies and procedures to cover DP and information security. Improved handling of personal information by volunteers, employees and office bearers within religious organisations.

Contact: David Freeland

7. International

7.1 Implications of the Schrems CJEU judgment on safe harbour for transfers of personal data from the EU to the USA

Latest developments:

The ICO has been working actively in the Article 29 working party to assess the implications of the Schrems judgment on transfers to the US. Although the judgment only declared the EC decision on the Safe Harbor framework invalid, the judgment also has implications for other mechanisms using legally support transfers to the US such Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs). The issue is therefore of considerable importance to data flows in the global economy, particularly the digital economy, and the use of online services such as cloud computing.

A key responsibility now lies with the European Commission to negotiate a Safe Harbor 2.0 with the US Government and gain agreement about acceptable reforms to US laws related to surveillance, to address the concerns raised by the CJEU.

In October the Article 29 Working Party agreed a statement that indicated that it would not be appropriate to take action to suspend transfers to the US at the present time and that work was needed to assess the impact of the judgment on BCRs and SCCs, plus assess the legal issues in the US, including the legal protections provided by US law against the standards required by EU law. A.29 indicated that would review the position at the end of January 2016. It also stressed the importance of the EC and US reaching a new agreement as soon as possible.

The ICO has been an active member of the various A.29 sub groups working on analysis to feed into the A.29 plenary 2/3 February. A.29 has held a number of hearings with US legal experts to inform their position. The ICO has also sought expert views from different sources.

In October a blog was published by David Smith updating data controllers on the ICO's view of the judgment and what would happen next. The key message has been - don't panic, assess and understand the basis of all your transfers to the US, wait for further guidance. The ICO also attended a roundtable with industry organised by DCMS.

Next steps – The A.29 plenary on 2/3 will decide on next steps. An external statement is likely to be published after that meeting. The

ICO will also provide an update and further guidance if necessary after this meeting.

Contact: Steve Wood

7.2 Work with the Home Office on UK borders matters and processing of passenger data

Latest developments:

The European Institutions have agreed a compromise text for the EU Passenger Name Record (PNR) Directive, which will require collection of PNR data from all flights arriving into and leaving the EU, as well as allow EU Member States to collect intra-EU PNR data should they wish to. Appropriate DP and privacy safeguards have been established in the text, such as the narrowing of the scope, the deletion and masking of data requirements and the reduced retention period. The ICO will continue to work with the Home Office and with the carriers covered, to implement the Directive.

The ICO is still awaiting the judgment of the Court of Justice of the European Union on the legality of the EU-Canada PNR agreement. The ruling will not be retrospective and so will not affect agreements made prior to the EU-Canada agreement being signed. The European Commission will not progress any other negotiations on the transfer of PNR data until this ruling is received.

Next steps:

Work with European counterparts in the Article 29 Working Party on the implementation of the Directive.

Contact: Hannah McCausland/Naomi Osborne-Wood

7.3 Europol/Eurojust/Customs/Eurodac/Schengen SIS II – large IT databases and information exchange at EU level for law enforcement purposes

Latest developments:

Europol: A new Regulation governing Europol has also been agreed. Liaison with the Home Office and the Europol National Unit will continue on how this Regulation will be implemented in the UK. The ICO recently undertook an Article 33(2) check of the national Europol system as part of our regulatory responsibilities.

SIS II: The ICO has recently undertaken a post-go live audit of the UK implementation of the Schengen Information System II. The ICO is aware of a number of subject access requests which have been made regarding data held in the SISII since the UK implementation.

Next steps:

- Work with the Home Office and the Europol Joint Supervisory Board to set up the new Cooperation Board under the incoming Regulation.
- Further liaison with the Europol National Unit to consolidate future individual access request processes.

Contact: Naomi Osborne-Wood

7.4 Article 29 (WP29) Working Party developments

Background and outcome:

Significant issues with implications for information rights (where these have not been referred to in other dedicated sections above) include:

- Adoption of Opinion 02/2015 on the code of conduct for Cloud computing.
- Statement on the implementation of the judgment of the Court of Justice of the European Union ruling of 6 October 2015 in the Maximilian Schrems vs the DP Commissioner case.
- Adoption of Opinion 03/2015 on the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.
- The first Cooperation workshop took place at the Working Party. This developed a common complaint form for a more effective transfer of individuals' complaints among DP authorities.

Next steps:

The ICO is considering the possibility to hold a workshop on a new topic of cooperation between DP authorities in 2016.

Contact: Hannah McCausland/Naomi Osborne-Wood

7.5 International Visitors

Latest developments:

The ICO has continued to receive international visitors to deepen our links with other DP and FOI agencies and to share our experience and understanding.

In the reporting period we have received visits from:

- A Canadian academic researching children's privacy.
- A Singapore delegation to discuss the EU DP reform package and big data.
- A Tunisian government and civil society delegation to discuss the implementation of their FOI law.

Contact: Naomi Osborne-Wood

7.6 Common Thread Network

Latest developments:

The ICO has continued to co-chair (with Canada's Office of the Privacy Commissioner) the Common Thread Network of DP Authorities across the Commonwealth.

Common Thread Network members met at the Amsterdam International Conference in October where focus was on using the network to help support individual authority capacity building through information and expertise exchange.

The Common Thread Network also called on the Commonwealth Heads of Government meeting (November 2015) to recognise the need to adopt legal frameworks that promote privacy rights and to ensure an open and secure internet as well as DP in accordance with the national laws of the states concerned. The ICO contacted the UK Government to promote the work of the Common Thread Network in this regard.

The Common Thread Network also embarked on work with another global network, the Global Privacy Enforcement Network, to improve information exchange among authorities which can help them face global and domestic challenges to individuals' rights more effectively.

Outcome:

The CHOGM Communique adopted in Valletta recognised the need to improve privacy legal frameworks and provided for future work to

support networks such as Common Thread in facilitating the sharing of information and building of capacity in these areas.

Next steps:

The ICO will work with Common Thread members to ensure that Governments across the Commonwealth follow up on the commitments made in the Communique to improve privacy and DP legal frameworks.

Contact: Hannah McCausland

7.7 International Enforcement Coordination

Latest developments and outcome:

Several key milestones in international enforcement cooperation have been reached, resulting in the finalisation of a number of tools that can be used in future to support privacy enforcement authorities in their cooperation on enforcement matters in future.

The Global Cross-Border Privacy Enforcement Arrangement came into force at the International Conference of DP and Privacy Commissioners in Amsterdam. This provides a framework for individual Authorities to shape their cooperation with any other Authority signed up to participate in the Arrangement.

The same conference also saw the presentation of a Handbook on Enforcement Cooperation (co-authored by the ICO with the Office of the Privacy Commissioner of Canada in the lead), which will be a useful reference tool in the ICO's own future enforcement practice.

The ICO also signed up to use the Global Privacy Enforcement Network (GPEN) Alert Tool which will allow the ICO to find out what other GPEN members are investigating or taking enforcement action against the same company, person or practices. It does not currently allow sharing of detailed confidential, non-public enforcement matters, nor does it allow the sharing of consumer complaints relating to privacy.

The alert uses the existing Consumer Sentinel Network (CSN) platform operated by the US Federal Trade Commission. The alert is separate from the rest of the CSN platform.

Next steps: ICO will hold the next International Annual Enforcement Event on March 21-22 in Alderley Edge, to progress Authorities' thinking on how best to use enforcement cooperation tools such as

the Arrangement and Handbook mentioned above and update the Handbook where necessary.

Contact: Hannah McCausland/Adam Stevens (Enforcement)

8. Enforcement

8.1 Anti-Spam Investigation Teams and Intelligence Hub

We issued eight civil monetary penalties totaling £731,000 for contraventions of the PECR. The largest fine in this period was £200,000 against Help Direct Ltd for sending unsolicited marketing text messages, and the lowest was a fixed penalty of £1,000 against Hutchison 3G for failing to report a personal data breach within the required time limit.

We also served three enforcement notices against; Mr Aurangzeb Iqbal, trading as The Hearing Clinic; Telecom Protection Service Ltd and Nuisance Call Blocker Limited, to compel future compliance with the law.

Two companies, HELM Ltd and UKMS Money Solutions Ltd, have appealed to the First-tier Tribunal against the monetary penalty notices issued against them.

The First-tier Tribunal refused an application by Optical Express (Westfield) Ltd for permission to appeal to the Upper Tribunal against its decision upholding the ICO's enforcement notice. Also, the Upper Tribunal refused an application for permission to appeal by Reactiv Media Ltd against the First-tier Tribunal's decision upholding the monetary penalty notice the ICO had served on them.

In late November, the ICO and the Ministry of Justice Claims Management Regulator held a 'week of action' in order to co-ordinate messaging around planned enforcement action, attend audits of claims management companies and publicise educational and awareness work. We also wrote to over 1,000 organisations which were registered for trading and sharing personal data, in order to better understand how people's personal data is being shared by organisations, and to identify non-compliance.

The ICO published the 'Stanley' data cycle animations, which aimed to help members of the public understand what may happen to their personal data, and to assist organisations in understanding compliance with the law. Stanley has now been viewed over 1,500 times.

We monitored six organisations this quarter which we believe represent risks in relation to adherence to PECR. We held seven compliance meetings with organisations in order to improve direct marketing practices, and four further meetings with charities, following concerns raised in July about their fundraising practices.

The meetings with the charities informed the ICO's ongoing investigation into whether those charities complied with the DPA and the PECR.

As a result of our investigations into compliance with the PECR we may identify breaches of related law.

Accordingly, on 22 December 2015 we prosecuted Swansea Accident Management Ltd for a non-notification offence. The company failed to attend Court. They were convicted in their absence and fined £500. They were ordered to pay costs of £669.85, a court charge of £180 and a victim surcharge of £50.

In this quarter we also prosecuted Space Systems Ltd for a non-notification offence. They pleaded guilty and received a fine of £500 (reduced from £750 for an early guilty plea), with £260 in costs, an either-way charge of £180, and a victim surcharge of £50. We prosecuted Direct Security Marketing Limited and its Director, Mr Anthony Pardo for similar offences; in total the parties were fined £1,184, received court charges of £360, costs of £621.86, and victim surcharges of £118. The fines were reduced for early guilty pleas.

Four further prosecutions for non-notification or related DPA offences are scheduled to take place in the next quarter.

We became one of the first participants to the Global Cross Border Enforcement Cooperation Arrangement at the International Conference in October. The ICO also presented on the International Enforcement Handbook, produced in partnership with the Office of Privacy Canada. Along with the newly launched GPEN Alert Tool, this provides us with the tools needed to work efficiently with other DP authorities internationally when sharing intelligence or cooperating on enforcement matters.

Work has begun on the 2016 GPEN Sweep, which will be led by the ICO. The 'Sweep' is a co-ordinated approach by international DP Authorities, in this case operating under the banner of GPEN, highlighting a specific privacy issue and making recommendations for action, as a result of the research conducted during the Sweep. Issues identified during the Sweep result in follow-up work such as outreach to organisations, analysis of privacy provisions or enforcement action.

Leading the 2016 GPEN Sweep is, therefore, a significant challenge and responsibility for the ICO. The topic will be decided in January,

with the 'Internet of Things' proposed. An internal steering group, led by the Intelligence Hub has been created.

Planning is underway for the first London Action Plan (LAP) Executive Committee meeting in January. This will involve representatives from Canada, the US, the Netherlands, New Zealand and the UK meeting in Wilmslow to finalise LAP's operational plan for 2016-18 to tackle spam. Work is also underway planning for the first ever LAP Sweep, led by the ICO and Canadian CRTC in 2016.

We have continued to publish the quarterly data security incident trends report as well as the monthly nuisance calls and messages threat assessments on our website. We routinely shared intelligence with other regulatory and law enforcement organisations to support our enforcement activity. We have developed new relationships by signing Memoranda of Understanding with the Insurance Fraud Bureau, the Solicitors Regulation Authority and the Fundraising Standards Board during the previous quarter.

We have presented on our priorities to CERT-UK and the Consumer Protection Partnership amongst others to highlight new opportunities for joint working. We have also sought to develop our existing relationships through reviewing our MoU with the Financial Conduct Authority and discussing our intelligence requirements with Ofcom ahead of reviewing our Letter of Understanding.

We have sought to improve our intelligence gathering capabilities through introducing a new whistleblowing procedure and briefing all ICO helpline staff to ensure individuals are given the correct advice and relevant information is captured. We have also begun a process to introduce specialist software to improve our analytical abilities, as well as improving the existing nuisance calls/texts reporting tool.

Next Quarter

We will continue to prioritise our investigations and activities to maintain focus on effective enforcement of the PECR, and progression of concerns received since the change of law on 6 April 2015.

We will report on our investigation of charities and whether they contravened the DPA and the PECR.

We will report on a 'mystery shopping' exercise the ICO has been conducting since April, with the aim of better understanding the

journey of some unsolicited marketing and how individuals can better protect their personal data.

We will continue to lead on the planning for the international GPEN Sweep 2016 and confirm the topic, with a view to the Sweep being conducted in April or May 2016.

We will chair and host the first ever London Action Plan (LAP) Executive Committee meeting and continue to jointly lead on planning the first ever LAP Sweep.

8.2 Civil Investigation Team

The team took the decision to create two sector specialist teams, and to implement a triage team on a permanent basis, following a successful pilot. These teams went live on 2 November 2015. It is hoped that this new team structure will allow staff to better develop sector expertise, to give greater consistency and oversight in terms of attendance at TCG meetings, and to provide greater opportunities to identify threats and trends.

The intake of new cases created in Q3 is as follows:

Cases in Q3	**443**

The closure rate of cases completed by Civil Enforcement teams in Q3 is as follows:

Cases out Q3	**451**

The team attained a 13% increase in case closures in Q3 when compared with Quarter 2.

323 cases are under active investigation at present. The team achieved a significant reduction in the number of cases awaiting allocation over Q3. The new triage process had a significant role to play in this.

Sector trends

	Q3	Total
Accountants	2	4
Audit/Inspections	0	0
Cent Gov	9	27
Charities	24	53
Clubs/Assoc	3	14
Courts/Justice	1	5
Credit Ref	0	0
Debt Collectors	2	9
Direct Marketing	0	1
Education	50	117
Estate Agents	2	6
Financial Advisors	7	15
Gen Business	45	88
Health	214	719
Housing	14	35
HR matters	1	2
Insurance	8	20
Internet	6	9
Leisure	11	15
Lenders	21	45
Local Gov	34	146
Mail order	0	0
Media	1	6
Motor Industry	0	2
MPs	1	3
Other	2	6
Other individuals	0	0
Pensions	2	5
Police & Crim records	18	52
Political parties	0	0
Prisons	0	0
Probation	0	1
Prof associations	0	2
Recruitment agencies	1	8
Regulators	4	21
Religious organisations	1	2
Retail	5	21
Social services	2	5
Solicitors/Barristers	20	52
Telecoms	4	10
Tenancy	0	0
Travel	3	7
Utilities	5	8
Total	523	1541

***this is derived from all cases risk assessed by the team – and includes those transferred to PID sector teams**

The most significant work stream for DPA breaches continues to be the Health sector. In the third quarter and as a percentage of the total intake of cases, health accounted for 41% of all those risk assessed.

In common with our experiences in 2014/2015 and in the first & second quarters, Local Government also continues to dominate. In Q3 just under 7% of the total intake related to the local government sector. However, despite both of these sectors continuing to represent significant areas of intake when expressed as a total number of case receipts; we actually received fewer reports from both of these areas in Q3 – a reduction of 46% for Local Government and a 27% reduction for Health compared with Q2. Though it is too early to confirm a definite trend, we will continue to keep this development under review.

Between February and November 2015, the team held a series of workshops across the country, aimed at improving DPA compliance in Local Authorities' Children's Services departments. These workshops were well received and will likely have contributed to a reduction in breaches in the local government sector.

There have however been some notable increases in the following sectors:

- Charities (+29%);
- Gen. Business (+62%);
- Lenders (+29%)

The increase in the General Business sector is of particular interest, and early indications suggest that this has been driven by an upswing in cyberattack incidents. These data loss incidents are becoming increasingly more complex in nature and therefore present new challenges for investigators and the ICO. This is also evidenced by the continued political and media interest in the subject. A recent House of Commons Culture, Media and Sport Committee, held on the 15 December 2015 heard evidence from Talk Talk and Vodafone amongst others, and recorded that GCHQ were dealing with 200 active cyberattacks on corporate Britain every month.

We continue to monitor the situation and to work with our stakeholders across Government to tackle this threat.

8.3 Monetary Penalties and formal regulatory action cases

Redacted

8.4 Other significant activity

We represented the Enforcement Department at the Welsh DPO conference in November and trialled a new interactive workshop on cyber incidents, which was well received.

A Lead Case Officer, along with colleagues from Good Practice and Strategic Liaison, represented the department at the Solicitors Regulation Authority annual compliance officer conference. We had previously identified solicitors and barristers as a threat area, and saw this as an opportunity to improve compliance in this sector.

There have been some developments in Operation Pyrite and whilst we continue to liaise with our DPA colleagues overseas in relation to this investigation, we have a new line of enquiry. We anticipate that this may lead us to share intelligence with other, non-DPA enforcement agencies.

Operation Juniper is to be closed as no substantive evidence of contemporary blacklisting has been uncovered. A communication strategy has been agreed and is in hand.

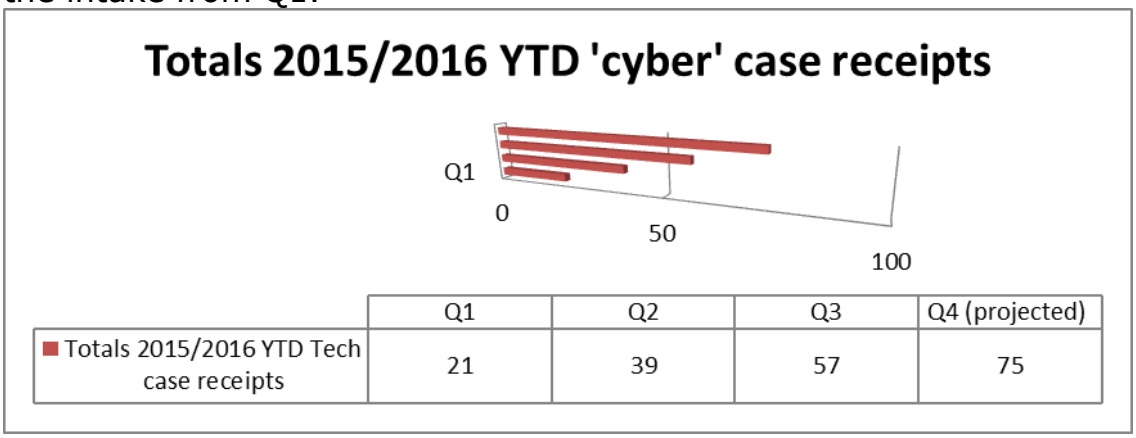
Google Inc appealed to the First-tier Tribunal against the Enforcement Notice requiring it to delist search results displayed following a search on a particular individual's name. The hearing of this appeal is unlikely to be heard before the first quarter of next year.

Tallington Lakes Leisure Park Ltd appealed to the First-tier Tribunal against an Information Notice served on it. This appeal is likely to be determined in Q4.

8.5 Q4 2015-2016

Cyberattacks continue to attract considerable political and media interest. '*Cyber Security: Protection of Personal Data Online Establishing World-Class Connectivity Throughout the UK'* is just one example of the current work Her Majesty's Government is undertaking on this topic. A recent House of Commons Culture, Media and Sport Committee on this topic, held on the 15 December 2015 and which heard evidence from Talk Talk and Vodafone amongst others, recorded that GCHQ were dealing with 200 active cyberattacks on corporate Britain every month.

Our projections suggest that we will receive our highest ever intake of 'cyber' cases in Q4 - we expect to receive more than three times the intake from Q1.



	Q1	Q2	Q3	Q4 (projected)
Totals 2015/2016 YTD Tech case receipts	21	39	57	75

To help absorb this demand we are submitting a business case for the recruitment of technical investigators to the team.

The team will have a presence at the ICO's annual DPPC conference in March at both the Information Cubes and the Q&A stand. We will also be running enforcement specific seminars.

9.6 Criminal Investigations Team:

Redacted

9. Performance Improvement

This quarter has again been a productive one for the Performance Improvement Teams. More of the performance information is held in the statistics but we have cleared more than intake on both FOI and DP casework (the first quarter that we have done so), and are well placed to increase output during the remainder of the financial year. We have completed considerable recruitment and are now fully staffed, increasing head count in the department to from 116 in July to 134 at the beginning of January. We have also been able to finalise 26 level C to level D promotions which will go some way to addressing migration issues that have hampered performance earlier in the year. There is an inevitable lead in time until new starters become fully productive but we are pleased with additions to the Department at the moment and optimistic for the future and lead up to year end.

FOI monitoring continues. The Ministry of Justice is being monitored. Returns indicate performance is still not up to a satisfactory level and if a significant improvement in timely replies to requests is not forthcoming then monitoring is likely to be extended and details of an improvement plan sought at the period. We continue to liaise closely with the Metropolitan Police Service in relation to its performance improvement action plan with regard to both FOI and DP performance. Whilst the DP front has seen significant improvement, progress on the FOI front is slow. We intend to meet Deputy Commissioner, Craig Mackey, early in 2016 to discuss the FOI situation further.

At the end of quarter 2 we wrote to all of the Northern Ireland Departments regarding FOI performance and provision of FOI statistics going forward, this is in the light of proposed departmental restructuring from April 2016. Since then all departments have responded and we are working closely with those whose performance needs improvement. We also met in December with the Office of the First Minister and deputy First Minister, the Department of Enterprise, Trade and Investment and the Department of Finance and Personnel (currently being formally monitored) to discuss performance and transitional plans.

The department is also working on ways in which it can report outcomes that are more aligned to our purpose. We are piloting a simple count of organisations that have altered practice as a result of our interventions or when the public have highlighted issues to be addressed. Likewise we are considering measures that show when useful information is placed into the public domain as a result of our decisions. We hope to incorporate that into standard statistical reporting in the new financial year.

Contact – Andy Laing

10. Policy Delivery

10.1 Independent Commission on FOI

Latest developments - The ICO submitted its evidence to the Commission on 17 November, followed by a meeting with the Commission Chair, Lord Burns, on 20 November. The ICO's evidence addressed the questions asked by the Commission, seeking to take an evidenced based approach and drawing on statistics and examples from ICO decision notices. The submission made the case that the protections provided by sections 35 and 36 are working in practice and evidence points towards a small percentage of cases where the application of the exemptions is overturned. On the veto the Commissioner accepted that the existence of a veto, which is used in exceptional cases, was a more proportionate response to concerns about the impact of the disclosure in certain cases compared to making sections 35 and 36 absolute. The submission also noted that flat fee charges could have a disproportionate impact on requesters. The ICO submission has been generally well received.

The UK media have been running a significant campaign in favour preserving FOIA for the last few months.

The Labour Party has also launched their own review of FOIA, with cross party involvement. The Commissioner also gave evidence to the review in December. The questions the Labour raises cover some of the same areas as the government sponsored review but also looks more at areas where the Act can be improved. At hearing the Commissioner explained his views on outsourcing and FOIA and how coverage of this area under FOIA needs to be improved.

Next steps – The Commissioner will provide formal oral evidence to the Commission at a hearing on 20 January. The Commission report is likely to follow shortly after these hearings. The Labour Review is likely to be published around the same time.

Contact: Steve Wood

10.2 FOI Practitioners' Conference 15 March 2015

Latest developments – For the first time the ICO will run an FOI Practitioners' conference. This will be on the day after the long standing DPPC. The FOI conference has already attracted 420 delegates. Lord Burns will give the keynote address to the conference as the Commission's report should have been published by then.

Contact: Steve Wood/Jo Pedder

10.3 Privacy Notices Code of Practice

A new version of the ICO privacy notices code of practice will be published for consultation in January. The Code has been updated to take account of developments in technology since the first version was developed in 2009, particularly the developments in mobile technology. The Code explains how tools such as just in time notices and dashboards can compliment traditional privacy notices and provide greater transparency and control to users. The consultation document also explains the ICO's plans for an interactive resource to support the code and asks for views of the different types of resource that could be developed, such as privacy notice generator tool, examples of dashboards.

Contact: Steve Wood/Jo Pedder

10.4 DP – Privacy Seals

Latest developments - work overseen by the Project Board continues. A contract has been awarded to a new company (Quadrant) for the seal logo design and marketing strategy. Different logo design options have been considered at meetings in December and January and Quadrant are running consumer research with on different design options in February. Further work is also being done to clarify the scope of the privacy seal schemes the ICO will seeking proposals on.

Next steps – The ICO plans to launch the call for applications to scheme providers later in 2016.

Contact: Steve Wood/Louise Byers

10.5 DP – Right to be forgotten

Latest developments – in November 2015 the ICO held a policy conference to discuss the implications of the Google Spain judgment on the so called "right to be forgotten". Three panel sessions were held exploring different implications of the judgment and wider issues arising from publishing personal information online. The panel sessions included various academic experts and lawyers, representatives from the BBC and Google, the Charity for rehabilitation – Unlock and the European DP Supervisor.

Next steps – a conference report will be published in January, highlighting key findings from the conference and areas where the ICO will do further policy work or where other stakeholders should take the lead. In particular the report will address the issue of how publishers can be notified of de-listing requests made to search engines, whilst ensuring this process complies with the DPA.

10.6 DP Technology Guidance

Work is ongoing with technology focussed guidance including a revision of the IT Security guide for SMEs, Encryption and Wi-Fi location tracking and the disclosure of personal data within datasets.

Outcome:

The guidance on the disclosure of personal data within datasets was published with a blog on the website on 13 November 2015. The guidance outlines the danger of personal data being hidden within certain file formats, typically released as part of an FOI request. Guidance on IT Security guide for SMEs, Encryption and Wi-Fi location tracking have been completed and passed to Internal Communications for an editorial review.

Future work:

Guidance on IT Security guide for SMEs, Encryption and Wi-Fi location tracking to be published on the website once editorial review has been completed. The IT Security guide for SMEs will also be printed in hard copy.

Contact: Simon Rice

10.7 Credit card fraud research

IRC approved a project proposal to conduct some research into individuals' attitudes and actual risks of harm as a result of payment card data being subject to unauthorised access as part of a data breach.

Outcome:

Following discussions with a payment card provider who indicated that they may be able to provide useful information to inform the research and therefore potentially avoid the need to consult external research this has not been possible and therefore the research shall continue as originally planned.

Future work:

Discussions with research agencies shall continue to determine appropriate questions and research topics in order to complete the research project.

Contact: Andrew Paterson

10.8 Technology Lab improvements

Approval from the IRC was given to spend a small amount of money to purchase additional equipment for the Technology Lab to update the mobile phone and network traffic capture capability in order to further investigate personal data processing in this area.

Outcome:

A new Android and Apple mobile phone have been purchased and work will continue to documents and investigate mobile apps to review personal data processed in addition to preparing to support the 2016 GPEN sweep.

Future work:

Once complete, the set-up shall be used to test other areas of interest such as Inter of Things devices or mobile apps from other business sectors as identified through the Emerging Technologies and Applications PAAG.

Contact: Simon Rice

10.9 Cookie sweep extension

In November 2014, the ICO coordinated the Article 29 Working Party conducted a sweep of European websites to assess the extent of the use of cookies. The ICO extended the methodology to review the impact that using a different web browser might have on the number and type of cookies set.

Outcome:

It was shown that usage of a different web browser or type of device (eg laptop vs a smart phone) can result in a different number and type of cookies set when visiting the same web page. There was a small but noticeable difference in the use of cookies on

mobile browsers when compared to desktop, with fewer cookies being set on the former.

Future work:

To publish and disseminate the results of the sweep in early 2016.
Contact: Simon Rice

10.10 General DP Regulation (GDPR)

Latest developments –

A final text of the GDPR was agreed between the EU institutions on 15 December, completing the trilogue process. A final text, including translations will now be completed and should be finally ratified during the first of half of 2016. The go-live date for the GDPR will therefore be sometime in the first half of 2018. Many of key features from previous drafts have been retained.

Key features of the text:

- Mandatory breach notification to DP authorities for data breaches that are likely to pose a risk to individuals.
- A nuanced definition of consent – unambiguous for all processing, explicit for processing sensitive personal data. Recitals make clear opt-out boxes are not acceptable.
- DPAs to provide prior authorisations for DP Impact Assessment that expose risk.
- Provisions on research that should be provide safeguards for individuals but also enable research to take place without disproportionate regulatory burdens.
- Risk based amendments will be of benefit to SMEs – eg from the requirement to designate a DP officer based risk/scale.
- A consistency mechanism for cross EU cases – the "One Stop Shop". Introduces the concept of a "Lead DPA".
- A role for privacy seals and certification to demonstrate compliance.
- Two levels in the fining regime for different types of breach -
    - 10M Euro or 2% of worldwide annual turnover
    - 20m Euro or 4% of worldwide annual turnover

Contact: Steve Wood

10.11 Directive on criminal justice and law enforcement cooperation

Latest developments:

Alongside the General DP Regulation, the trilogue process has agreed a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In the UK, the Directive will apply to those data controllers processing personal data for those EU JHA measures relating to judicial cooperation in criminal matters and police cooperation that the UK re-joined on 1 December 2014.

Outcome: The ICO has invited the Home Office to its event on the implementation of the EU reform due to take place in January.

Next steps:

The ICO will continue to work closely with DCMS and the Home Office on the implementation of the reform package. Hold the ICO event on the EU DP reform package.

Contact: Naomi Osborne-Wood